The attractive application of geometric objects known as “caps” to research in error-correcting codes (a popular topic in information theory) led to the proposal for funding during the 2011-2012 academic year. The project has been an on-going effort throughout that period and has led to an article suitable for submission in a peer-reviewed professional journal.

In the spring of 2011, I began work on the project with two colleagues, one from Regent University in VA and another who works as a private contractor for the Department of Defense. We arranged several meetings in Fredericksburg and were able to do considerable work on the project early on. When working in finite spaces, there is always an associated number, called the “order”, that describes the numbers of points on a line as well as many other characteristics of the space. When the order, $q$, is odd, sometimes the structure of the underlying space is quite different from the case when $q$ is even. Such was the situation in our project and we discovered this very early in the research. We were able to prove theorems in the odd case only. I am happy to report that the even case did eventually work out as well, but this took us well into the fall semester to come to fruition.

In the end, the three of us were able to give sufficient conditions for when sets of conics in the affine plane could be joined together to lift to caps of a higher dimensional space. The proofs were very different in the even and odd cases. The sets of conics giving our desired construction were also able to be pieced together almost to form a partition of the spaces (we had to delete one point). Our efforts resulted in a paper that we submitted to the journal *Finite Fields and their Applications*, a leading journal for the broad area of algebraic combinatorics. The article is attached to this report.

I appreciate the funds UMW provided for me to complete this project, one that I have been eyeing for several years. The university has been generous in awarding grant money to support my efforts as a research mathematician and it is satisfying that I have been able to produce publications on a regular basis in return.
Generalized Pellegrino caps

Jeremy M. Dover Keith E. Mellinger∗† Kenneth L. Wantz

January 4, 2012

Abstract

A cap in a projective or affine geometry is a set of points with the property that no line meets the set in more than two points. Barwick, et al. (Conics and caps. J. Geom., 100:15–28, 2011) provide a construction of caps in $PG(4, q)$ by “lifting” arbitrary caps of $PG(2, q^2)$, such as conics. In this article, we extend this construction by considering when the union of two or more conics in $AG(2, q^2)$ can be lifted to a cap of $AG(4, q)$ using a similar coordinate transformation. In particular, the authors investigate a family of caps of size $2(q^2 + 1)$ in $AG(4, q)$ for all prime powers $q > 2$, of which the celebrated Pellegrino 20-cap in $AG(4, 3)$ is the smallest example.

Keywords: projective plane, cap, conic

AMS subjects: 51E21, 51E22

1 Introduction

A cap in a projective or affine geometry is a set of points with the property that no line meets the set in more than two points. The study of caps in finite affine and projective spaces is motivated by a connection to various classical problems, including certain construction problems for optimal linear codes and partitioning problems in finite geometric spaces. In many of these applications, finding the maximal size of a cap in a finite geometric space is a problem of particular interest.

In a projective or affine plane of order $q$, the maximal size of a cap is bounded by $q + 1$ if $q$ is odd, or $q + 2$ if $q$ is even. These bounds are achieved in the Desarguesian and many other
planes, though there do exist planes where the maximal cap is smaller than these bounds, for example the dual derived semifield plane of order 16. (See Penttila, et al. [10].)

There exist bounds on the maximal size of a cap in higher-dimensional geometries, but exact values are known in only a very few small cases. In $AG(4, q)$ or $PG(4, q)$, the cases of most interest in this paper, the maximal size of a cap is $O(q^3)$. If $q \geq 8$ is even, the maximal size of a cap in $PG(4, q)$ is less than or equal to $q^3 - q^2 + 6q - 3$ (Hirschfeld and Storme [8]). Both bounds are non-constructive, and the best-known caps are significantly smaller than these bounds. But one celebrated result in this direction is due to Pellegrino [9], who showed that the maximal size of a cap in both $AG(4, 3)$ and $PG(4, 3)$ is 20. Pellegrino’s construction provides one type of 20-cap in $AG(4, 3)$ and nine types of 20-caps in $PG(4, 3)$ (see Hill [6]).

Tucker [11] provides an interesting analysis of Pellegrino’s cap in $AG(4, 3)$. Viewing $GF(9)$ as a two-dimensional vector space over $GF(3)$ with basis $\{1, \epsilon\}$, there is a natural bijection between the points of $AG(4, 3)$ and the points of $AG(2, 9)$, via $(a, b, c, d) \leftrightarrow (a + be, c + de)$. Looking at the image of a Pellegrino cap in $AG(4, 3)$ under this bijection, Tucker noticed that the resulting set in $AG(2, 9)$ is the union of two conics, each conic consisting exclusively of interior points of the other conic.

This observation begs the question of whether the Pellegrino construction can be generalized through “lifting” sets of conics to higher-dimensional affine geometries. Barwick, et al. [1], show that any cap in $AG(2, q^2)$, and particularly a single conic, lifts to a cap in $AG(4, q)$. Hence, they are able to construct caps of size $q^2 + 1$ in $AG(4, q)$ for $q$ odd, and size $q^2 + 2$ for $q$ even. In this article, we exhibit an infinite family of caps which we call generalized Pellegrino caps that result from “lifting” the union of a pair of disjoint conics from $AG(2, q^2)$ to $AG(4, q)$ for all $q > 2$. We also explore the possibility of extending these pairs to larger sets of conics.

2 The lifting process

Let $q$ be a prime power, and consider the classical affine spaces $\pi = AG(2, q^2)$ and $\Sigma = AG(4, q)$. Let $\{1, \epsilon\}$ be a basis of $GF(q^2)$ considered as a two-dimensional vector space over $GF(q)$, and define the mapping $\psi : \pi \to \Sigma$ via $\psi(a + be, c + de) = (a, b, c, d)$. The map $\psi$ is obviously a bijection from the points of $\pi$ onto the points of $\Sigma$. Given a set of points $S \subset \pi$, we say that $S$ lifts to the point set $\psi(S)$ of $\Sigma$.

In order to construct caps in $\Sigma$ by lifting sets of points from $\pi$, we need to understand the pre-images of lines under $\psi$. Given two points $P = (p_0, p_1, p_2, p_3)$ and $Q = (q_0, q_1, q_2, q_3)$
in Σ, the line ℓ containing them consists of exactly the affine linear combinations of their coordinate vectors over GF(q); i.e., \( ℓ = \{ tP + (1-t)Q : t \in GF(q) \} \). Thus the pre-image of ℓ under \( ψ \) consists of the points \( \{ tP + (1-t)Q : t \in GF(q) \} \), where \( P = (p_0 + p_1 \epsilon, p_2 + p_3 \epsilon) \) and \( Q = (q_0 + q_1 \epsilon, q_2 + q_3 \epsilon) \). In the projective completion of the affine plane \( π \), it is straightforward to show that this pre-image forms the affine portion of a Baer subline that meets the line at infinity in a point, hence we refer to these sets of size \( q \) as affine Baer sublines in \( π \).

The condition for a set \( S \) of points in \( π \) to lift to a collinear set in \( Σ \) is for the set to be Baer-collinear in \( π \); i.e., the points of \( S \) lie together in an affine Baer subline of \( π \). It follows that a set \( S \) in \( π \) such that no three points are Baer-collinear will lift to a cap of \( Σ \); we call such a set \( S \) a Baer-cap. From the definition, a set of points \( S \) in \( π \) lifts to a cap of \( Σ \) if and only if \( S \) is a Baer-cap.

We need to determine when the union of two disjoint Baer-caps is a Baer-cap. The following definition and proposition provide necessary and sufficient conditions for this to occur.

**Definition 2.1.** Let \( S \) and \( T \) be disjoint Baer-caps in \( π \). The Baer-cap \( T \) is said to be \( S \)-good if no affine Baer subline meeting \( S \) also meets \( T \) in two points.

**Proposition 2.2.** Suppose \( S \) and \( T \) are disjoint Baer-caps in \( π \). The set \( S \cup T \) is a Baer-cap of \( π \) if and only if \( S \) is \( T \)-good and \( T \) is \( S \)-good.

**Proof.** Let \( S \) and \( T \) be disjoint Baer-caps in \( π \). Suppose first that \( S \cup T \) is a Baer-cap, and let \( ℓ \) be an affine Baer subline meeting \( S \) (resp. \( T \)). Then \( ℓ \) meets \( S \cup T \) in at most two points, meaning \( ℓ \) can meet \( T \) (resp. \( S \)) in at most one point. Hence every affine Baer subline meeting \( S \) (resp. \( T \)) meets \( T \) (resp. \( S \)) in at most one point, implying \( T \) is \( S \)-good (resp. \( S \) is \( T \)-good). Conversely if \( S \cup T \) is not a Baer-cap, there exists an affine Baer subline \( ℓ \) meeting \( S \cup T \) in at least three points. Since \( S \) and \( T \) are Baer-caps, \( ℓ \) must meet either \( S \) or \( T \) in two points, and the other in at least one point. This forces either \( T \) not to be \( S \)-good or vice versa. \( \square \)

### 3 A linear pencil of conics

As noted in Tucker [11], the Pellegrino cap in \( AG(4,3) \) can be obtained by lifting the union of a pair of disjoint ellipses \( C \) and \( D \) in \( AG(2,9) \). These two ellipses are caps, and thus necessarily Baer-caps. By Proposition 2.2, since their union is a Baer-cap, \( C \) must be \( D \)-good and \( D \) must be \( C \)-good. We call such Baer-caps *mutually good.*
Tucker also notes that the conics $C$ and $D$ are mutually interior; i.e., $C$ consists wholly of interior points of $D$ and vice versa. From Dover and Mellinger [3], this suggests that we consider ellipses contained in the linear pencil of conics $P = \{C_\lambda : \lambda \in GF(q^2)\}$, where $C_\lambda$ is defined via

$$C_\lambda = \{(x, y) \in \pi : f(x, y) = \lambda\}$$

for some fixed irreducible quadratic form $f$. Following Hirschfeld [7], we may always assume $f(x, y) = x^2 + xy + ey^2$ for some $e \in GF(q^2)$ such that $x^2 + x + e$ is irreducible over $GF(q^2)$.

Group actions on the pencil $P$ play an essential role in identifying pairs of ellipses whose union is a Baer-cap. The automorphism group of $\pi$ is the group of two-dimensional affine semi-linear transformations over $GF(q^2)$, but here we are only interested in linear transformations which fix $C_0$ (the point $(0, 0)$). Therefore, we restrict our attention to the subgroup of automorphisms induced by $2 \times 2$ matrices over $GF(q^2)$ acting on point-coordinate vectors via right multiplication.

**Proposition 3.1.** Let $\pi = AG(2, q^2)$, and let $P = \{C_\lambda : \lambda \in GF(q^2)\}$ be the linear pencil of conics with $C_\lambda = \{(x, y) \in \pi : x^2 + xy + ey^2 = \lambda\}$, where $x^2 + x + e$ is irreducible. Define

$$\phi_{a,b} = \begin{bmatrix} a + b & -b \\ eb & a \end{bmatrix}.$$ 

1. The automorphisms of $\pi$ induced by $\{\phi_{a,b} : a, b \in GF(q^2), a, b \text{ not both } 0\}$ form a group $G$ of order $q^4 - 1$ leaving the pencil $P$ invariant.

2. If the automorphism $\phi_{a,b}$ maps $C_1$ onto $C_\mu$, then $\phi_{a,b}$ maps $C_\lambda$ onto $C_\mu \lambda$.

3. The group $G$ acts transitively on the ellipses in $P$.

4. The group $G$ has a subgroup $G_1$ of order $q^2 + 1$ that leaves each ellipse of $P$ invariant and acts sharply transitively on the points of each ellipse.

**Proof.** The determinant of the matrix representation of $\phi_{a,b}$ is $a^2 + ab + eb^2$, which is nonzero for all $a, b \in GF(q^2)$ except $a = b = 0$. Hence each $\phi_{a,b} \in G$ induces an automorphism of $\pi$. That $G$ is closed under composition and has order $q^4 - 1$ are easy calculations. To see that $G$ leaves $P$ invariant, let $(x, y)$ be any point of $C_\lambda$, whence $x^2 + xy + ey^2 = \lambda$. The image of $(x, y)$ under $\phi_{a,b}$ is $(ax + bx + eby, -bx + ay)$. This point lies in some $C_\lambda'$, which can be
determined by calculating:

\[
\lambda' = (ax + bx + eby)^2 + (ax + bx + eby)(ay - bx) + e(ay - bx)^2 
\]

\[
= (a^2 + 2ab + b^2 - ab - b^2 + eb^2)x^2 
\]

\[
+ (2eab + 2eb^2 + a^2 + ab - eb^2 - 2eab)xy 
\]

\[
+ (e^2b^2 + eab + ea^2)y^2 
\]

\[
= (a^2 + ab + eb^2)(x^2 + xy + ey^2) 
\]

\[
= (a^2 + ab + eb^2)\lambda. 
\]

So \(\phi_{a,b}\) maps every point of \(C_\lambda\) onto \(C_{(a^2+ab+eb^2)\lambda}\), implying \(G\) leaves the pencil \(P\) invariant. Moreover this calculation shows that if \(\phi_{a,b}\) maps \(C_1\) onto \(C_\mu\), then \(\phi_{a,b}\) maps \(C_\lambda\) onto \(C_{\mu\lambda}\).

To show the transitivity properties of \(G\), we first show that \(G\) acts sharply transitively on the set \(\pi' = \pi \setminus \{(0,0)\}\). Since the size of the \(G\) is the same as the size of the set \(\pi'\) on which it acts, we only need to show that no non-identity element of \(G\) has a fixed point. For \(\phi_{a,b}\) to have a fixed point, there must exist some \(x, y \in GF(q^2), x, y\) not both zero, such that \((x, y)\phi_{a,b} = (x, y)\). This would force \((ax + bx + eby, -bx + ay) = (x, y)\), which implies \((a+b-1)(a-1) - (eb)(-b)\) must be zero. But this simplifies to \((a-1)^2 + (a-1)b + eb^2 = 0\), which forces \(a = 1\) and \(b = 0\), making \(\phi_{a,b}\) the identity. Thus every non-identity element of \(G\) is fixed-point free on \(\pi'\), implying \(G\) acts sharply transitively on this set.

The transitivity of \(G\) on \(\pi'\), combined with the fact that \(G\) leaves the pencil \(P\) invariant, shows immediately that \(G\) is transitive on the ellipses in \(P\). Let \(G_1\) be the “special linear” subgroup of \(G\); i.e. \(G_1 = \{\phi_{a,b} : a^2 + ab + eb^2 = 1\}\). Clearly \(G_1\) leaves each ellipse of \(P\) invariant; moreover any element of \(G\) that leaves any ellipse of \(P\) invariant must lie in \(G_1\). Thus by the orbit-stabilizer theorem, \(G_1\) must have order \(q^2 + 1\), which is conveniently equal to the number of points in each ellipse of \(P\). Since we already know every non-identity element of \(G_1\) is fixed-point free, we have that \(G_1\) acts sharply transitively on the points of each ellipse in \(P\). \(\square\)

### 4 Mutually good ellipses in \(AG(2, q^2)\)

In this section we wish to identify pairs of mutually good ellipses \(C_\mu\) and \(C_\lambda\) lying in the linear pencil \(P\) of \(AG(2, q^2)\). We first note that by Proposition 3.1, Part 3, we may assume without loss of generality that \(\mu = 1\) since the group \(G\) is transitive on ellipses in \(P\). Moreover by Proposition 3.1, Part 2, showing that \(C_1\) is \(C\)-good is equivalent to showing that \(C_{\lambda^{-1}}\) is \(C_1\)-good. Thus our focus in this section is on identifying values \(\lambda\) such that \(C_\lambda\) is \(C_1\)-good.
For a fixed, nonzero value of $\lambda$, how does one determine if $C_\lambda$ is $C_1$-good? From the definition, $C_\lambda$ is $C_1$-good if and only if there exists no affine Baer subline meeting $C_1$ and containing two points of $C_\lambda$. From Proposition 3.1, the automorphism group $G_1$ leaves each ellipse in $\mathcal{P}$ invariant while permuting the points of each ellipse. Hence there is no affine Baer subline meeting $C_1$ and containing two points of $C_\lambda$ if and only if there is no affine Baer subline meeting $C_1$ in the point $(1,0)$ and containing two points of $C_\lambda$.

**Theorem 4.1.** The ellipse $C_\lambda$, $\lambda \notin \{0,1\}$, is $C_1$-good if and only if for all $a,b \in GF(q^2)$ such that $\frac{2a+b}{a^2+ab+eb^2} \in GF(q) \setminus \{-1,-2\}$, $\lambda \neq (a+1)^2 + (a+1)b + eb^2$.

**Proof.** An ellipse $C_\lambda$, $\lambda \notin \{0,1\}$, is $C_1$-good if and only if there exists no affine Baer subline through $(1,0)$ containing two points of $C_\lambda$. Let $R = (a+1,b)$ be an arbitrary point of $C_\lambda$ from which $\lambda = (a+1)^2 + (a+1)b + eb^2$. The affine Baer subline $\ell_{a,b}$ containing $(1,0)$ and $R$ consists of the points $\{(ta+1, tb) : t \in GF(q)\}$ and meets $C_\lambda$ in two points if and only if $\lambda = (ta+1)^2 + (ta+1)b + e(tb)^2$ has a solution $t \in GF(q)$ such that $t \notin \{0,1\}$. (If $t = 0$, then $\lambda = 1$, which is not of interest.)

Manipulating the two equations for $\lambda$ yields $(t^2 - 1)(a^2 + ab + eb^2) + (t - 1)(2a + b) = 0$, and since we are looking for solutions distinct from $t = 1$ we must have $t = -1 - \frac{2a+b}{a^2+ab+eb^2}$. (We can safely divide by $a^2 + ab + eb^2$ since $a, b$ are not both zero.) Thus the affine Baer subline $\ell_{a,b}$ meets $C_\lambda$ in two points if and only if this value for $t \notin \{0,1\}$ lies in $GF(q)$, which occurs if and only if $\frac{2a+b}{a^2+ab+eb^2} \in GF(q) \setminus \{-1,-2\}$.

Therefore, there exists no affine Baer subline through $(1,0)$ containing two points of $C_\lambda$ if and only if for all $a,b \in GF(q^2)$ not both zero with $\frac{2a+b}{a^2+ab+eb^2} \in GF(q) \setminus \{-1,-2\}$, $\lambda \neq (a+1)^2 + (a+1)b + eb^2$, as claimed. \qed

The set of values of $\lambda$ satisfying the conditions in Theorem 4.1 seems difficult to pin down completely, but we are able to produce examples for every prime power $q > 2$. At this point, we need to distinguish between the even and odd order cases; the odd case will be handled first.

**Theorem 4.2.** Let $q$ be an odd prime power and let $\lambda$ be an element of the subfield $GF(q)$ of $GF(q^2)$ such that $\sqrt{\lambda}$ lies in $GF(q^2) \setminus GF(q)$. Then, $C_\lambda$ is $C_1$-good.

**Proof.** Letting $\lambda$ be as claimed, assume by way of contradiction that $C_\lambda$ is not $C_1$-good. Then by Theorem 4.1 there exist $a,b \in GF(q^2)$ with $\frac{2a+b}{a^2+ab+eb^2} \in GF(q) \setminus \{-1,-2\}$ such that $\lambda = (a+1)^2 + (a+1)b + eb^2$, which can be written as $\lambda = a^2 + ab + eb^2 + 2a + b + 1$. The condition on $a$ and $b$ implies that $2a+b = \mu(a^2 + ab + eb^2)$ for some $\mu \in GF(q) \setminus \{-1,-2\}$,
allowing us to write $\lambda - 1 = (1 + \mu)(a^2 + ab + eb^2)$. As $\lambda - 1$ and $1 + \mu$ are both in $GF(q)$ and nonzero, $a^2 + ab + eb^2 \in GF(q)$, which also shows $2a + b \in GF(q)$.

Since $a^2 + ab + eb^2 \in GF(q)$, $4a^2 + 4ab + 4eb^2 \in GF(q)$ as well, which can be rewritten as $4a^2 + 4ab + b^2 + (4e - 1)b^2 \in GF(q)$. Noting that $4a^2 + 4ab + b^2 = (2a + b)^2 \in GF(q)$, we have $(1 - 4e)b^2 \in GF(q)$. The discriminant of the irreducible polynomial $x^2 + x + e$ is $1 - 4e$, which is a nonsquare in $GF(q^2)$. If $b^2$ were nonzero, we would have $(1 - 4e)b^2 \in GF(q)$ being a nonsquare in $GF(q^2)$, a contradiction which forces $b = 0$. The fact that $b = 0$, combined with $2a + b \in GF(q)$, shows $a \in GF(q)$. But $b = 0$ implies $\lambda = (a + 1)^2$, forcing $\lambda$ to have a square root in $GF(q)$, a final contradiction.

**Corollary 4.3.** Let $q$ be an odd prime power and let $\lambda$ be an element of the subfield $GF(q)$ of $GF(q^2)$ such that $\sqrt{\lambda}$ lies in $GF(q^2) \setminus GF(q)$. Then $C_1 \cup C_\lambda$ is a Baer-cap.

**Proof.** By Theorem 4.2, $C_\lambda$ is $C_1$-good. But note that $\lambda^{-1}$ also satisfies the conditions of Theorem 4.2, implying $C_{\lambda^{-1}}$ is also $C_1$-good. It then follows that $C_1$ is $C_\lambda$-good. Proposition 2.2 then shows that $C_1 \cup C_\lambda$ is a Baer-cap.

For some small odd prime powers $q$, there exist values for $\lambda$ other than those in Theorem 4.2 which satisfy the conditions of Theorem 4.1. But for $q > 5$, computational results seem to indicate that the set is complete.

For the even order case, there are two separate families of “good” values of $\lambda$.

**Theorem 4.4.** Let $q$ be an even prime power and suppose $\lambda^{q-1} = 1$ or $\lambda^{q+1} = 1$, with $\lambda \neq 1$. Then $C_\lambda$ is $C_1$-good.

**Proof.** Suppose that $\lambda$ is as claimed and assume by way of contradiction that $C_\lambda$ is not $C_1$-good. Then by Theorem 4.1 and using the fact that $GF(q)$ has even characteristic, there exist $a, b \in GF(q^2)$ with $\frac{b}{a^2 + ab + eb^2} \in GF(q) \setminus \{0, 1\}$ such that $\lambda = a^2 + ab + eb^2 + b + 1$. Since $b \neq 0$, we can write $b = \mu(a^2 + ab + eb^2)$ for some nonzero $\mu \in GF(q)$, whence $\lambda = (1 + \mu)(a^2 + ab + eb^2) + 1$. We calculate $\lambda^q = (1 + \mu)(a^2 + ab + eb^2)^q + 1$.

Suppose first that $\lambda^{q-1} = 1$. Then $\lambda^q = \lambda$, or $(1 + \mu)(a^2 + ab + eb^2)^q + 1 = (1 + \mu)(a^2 + ab + eb^2) + 1$, and since $1 + \mu \neq 0$ (otherwise $\lambda = 1$), it follows that $a^2 + ab + eb^2 \in GF(q)$. This forces $b \in GF(q) \setminus \{0\}$, so we can write $e^2 + c + e \in GF(q)$, where $c = a/b$. As $e^2 + c + e \in GF(q)$, the absolute trace $Tr(e^2 + c + e)$ from $GF(q^2)$ to $GF(2)$ must be 0. Since $Tr(e^2) = Tr(e)$, the additivity of trace implies $Tr(e) = 0$. But recall that $q$ is even and the polynomial $x^2 + x + e$ is irreducible, so $Tr(e)$ must be 1. This is the needed contradiction for this case.
Suppose now that \( \lambda^{q+1} = 1 \), or \( \lambda^q = \lambda^{-1} \). Writing \( \lambda = a^2 + ab + eb^2 + b + 1 \) and noting \( b \neq 0 \), we can recast this as \( \lambda = (c^2 + c + e)b^2 + b + 1 \), where \( c = a/b \). Since \( \frac{b}{\lambda^2 + \lambda + b^2} \in GF(q) \) is nonzero, its reciprocal also lies in \( GF(q) \), which can be written as \( \nu = (c^2 + c + e)b \in GF(q) \). We then have \( \lambda + 1 = (c^2 + c + e)b^2 + b \) which immediately implies that \( (\lambda + 1)(c^2 + c + e) = \nu^2 + \nu \). This shows that \( (\lambda + 1)(c^2 + c + e) \in GF(q) \). Thus we can calculate

\[
(\lambda + 1)^q(c^2 + c + e)^q = (\lambda + 1)(c^2 + c + e)
\]

\[
\Rightarrow (\lambda^{-1} + 1)(c^2 + c + e)^{q^{-1}} = \lambda + 1
\]

\[
\Rightarrow (c^2 + c + e)^{q^{-1}} = \lambda.
\]

The last step uses the fact that \( \lambda \neq 1 \).

Since \( (\lambda + 1)(c^2 + c + e) = \nu^2 + \nu \), we substitute to obtain \( (c^2 + c + e)^q + (c^2 + c + e) = \nu^2 + \nu \). The left-hand side of this equation is the trace of \( c^2 + c + e \) from \( GF(q^2) \) to the subfield \( GF(q) \). Now consider the absolute trace of both sides of this equality from \( GF(q) \) to \( GF(2) \). By the transitivity of trace, the left-hand side of the equation is the absolute trace of \( c^2 + c + e \) from \( GF(q^2) \) to \( GF(2) \). On the right-hand side, both \( \nu \) and \( \nu^2 \) have the same absolute trace, meaning \( Tr(c^2 + c + e) = 0 \). As above, this forces \( Tr(e) = 0 \), but we know \( Tr(e) = 1 \), our desired contradiction.

Similar to Corollary 4.3, the following corollary of Theorem 4.4 shows that the union of two ellipses is a Baer-cap, but also provides a small extension in one case.

**Corollary 4.5.** Let \( q \) be an even prime power, and let \( \lambda \neq 1 \) satisfy either \( \lambda^{q-1} = 1 \) or \( \lambda^{q+1} = 1 \). Then, \( C_1 \cup C_\lambda \) is a Baer-cap. Moreover in the case where \( \lambda^{q+1} = 1 \), \( C_1 \cup C_\lambda \cup \{(0,0)\} \) is a Baer-cap.

**Proof.** Following the proof of Corollary 4.3, that \( C_1 \cup C_\lambda \) is a Baer-cap follows from the fact that the sets \( \{ \lambda : \lambda^{q-1} = 1 \} \) and \( \{ \lambda : \lambda^{q+1} = 1 \} \) are both closed under field inversion. To show that \( C_1 \cup C_\lambda \cup \{(0,0)\} \) is a Baer-cap when \( \lambda^{q+1} = 1 \), we note that \( S = C_1 \cup C_\lambda \) and \( T = \{(0,0)\} \) are disjoint Baer-caps, and that \( T \) is vacuously \( S \)-good. By Proposition 2.2, we need only show that no affine Baer subline through \( (0,0) \) meets \( C_1 \cup C_\lambda \) in two points.

If \( (x, y) \) is a point of \( C_\mu \), then the affine Baer subline \( \ell \) containing \( (0,0) \) and \( (x, y) \) consists of the points \( \{(tx, ty) : t \in GF(q)\} \), and it is trivial to see that \( (tx, ty) \) lies in \( C_\mu \). This shows that \( \ell \) meets any ellipse \( C_\mu \) in at most one point and, moreover, \( \ell \) meets \( C_\nu \) if and only if \( \nu \) is a \( GF(q) \)-multiple of \( \mu \). Since \( \lambda^{q+1} = 1 \) and \( \lambda \neq 1 \), \( \lambda \) is not in \( GF(q) \), meaning that no affine Baer subline through \( (0,0) \) can meet both \( C_1 \) and \( C_\lambda \). Thus no affine Baer subline through \( (0,0) \) can meet \( C_1 \cup C_\lambda \) in two points, finishing the proof. 

\[ 9 \]
In the even case, computational results again suggest that the values of $\lambda$ in Corollary 4.5 are the only ones that satisfy the conditions of Theorem 4.1; there are no exceptions for small values of $q$.

Finally, we can summarize the results of this section with the following theorem.

**Theorem 4.6.** Let $q > 2$ be a prime power. Then $AG(4, q)$ has a cap of size $2(q^2 + 1)$ obtained by lifting a pair of disjoint ellipses from $AG(2, q^2)$. If $q$ is even, then there also exists a cap of size $2q^2 + 3$ in $AG(4, q)$ obtained by adding a point to a pair of disjoint ellipses lifted from $AG(2, q^2)$.

**Proof.** For odd $q$, $GF(q)$ has $\frac{1}{2}(q - 1)$ nonsquares, meaning that there is at least one $\lambda$ satisfying the conditions of Corollary 4.3 in $AG(2, q^2)$. Hence $AG(2, q^2)$ has a Baer-cap consisting of a pair of disjoint ellipses, which can be lifted to a cap of size $2(q^2 + 1)$ in $AG(4, q)$.

For even $q$, $GF(q^2) \setminus \{1\}$ contains $q - 2$ values for $\lambda$ such that $\lambda^{q - 1} = 1$, and $q$ values for $\lambda$ such that $\lambda^{q + 1} = 1$, meaning there is at least one $\lambda$ satisfying the conditions of Corollary 4.5. The result follows as for the odd case. \[ \Box \]

The smallest cap in this family, when $q = 3$, is the Pellegrino 20-cap in $AG(4, 3)$, hence the designation “generalized Pellegrino caps.”

## 5 Mutually good parabolas in $AG(2, q^2)$

Given the success in identifying pairs of ellipses in $\pi = AG(2, q^2)$ whose union can be lifted to a cap in $\Sigma = AG(4, q)$, it is reasonable to look for other conics that can be lifted as well. In this section, we investigate the linear pencil consisting of conics

$$D_\mu = \{(x, y) \in \pi : x = y^2 + \mu\}$$

for all $\mu \in GF(q^2)$, for $q$ an odd prime power. Note that each $D_\mu$ is a parabola in $\pi$.

As with the pencil of ellipses, we first need a result describing the group action on this pencil.

**Proposition 5.1.** Let $\pi = AG(2, q^2)$, and let $Q = \{D_\mu : \mu \in GF(q^2)\}$ be the linear pencil of conics with $D_\mu = \{(x, y) \in \pi : x = y^2 + \mu\}$. Define an affine transformation $\tau_{a, b}$ via

$$(x, y)\tau_{a, b} = \left(x + ay + \frac{a^2}{4} + b, y + \frac{a}{2}\right)$$

which is an automorphism of $\pi$ for all $a, b \in GF(q^2)$. 
1. The automorphisms of $\pi$ induced by $\{\tau_{a,b} : a, b \in GF(q^2)\}$ form a group $H$ of order $q^4$ leaving the pencil $Q$ invariant.

2. The automorphism $\tau_{a,b}$ maps $D_\mu$ onto $D_{\mu+b}$.

3. The group $H$ acts transitively on the parabolas in $Q$.

4. The group $H$ has a subgroup $H_1$ of order $q^2$ that leaves each parabola of $Q$ invariant and acts sharply transitively on the points of each parabola.

Proof. The proof of this proposition is very similar to the proof of Proposition 3.1, therefore we minimize the computational details. Part 1 of the proposition is proven by recognizing that $\tau_{a,b}\tau_{c,d} = \tau_{a+c,b+d}$, and Part 2 is a rapid calculation as well. Part 2 then immediately shows that $H$ is transitive on the parabolas in $Q$. Defining $H_1 = \{\tau_{a,0} : a \in GF(q^2)\}$, it is clear that $H_1$ is a subgroup of $H$ of order $q^2$ and that $H_1$ leaves each parabola in $Q$ invariant. The point $(x,y)$ is fixed by $\tau_{a,0}$ if and only if $(x+ay+a^2/4, y+\frac{a}{2}) = (x,y)$, which forces $a = 0$. Thus every nonidentity element of $H_1$ is fixed-point free, implying that $H_1$ acts sharply transitively on the $q^2$ points of each parabola in $Q$. 

As discussed for the ellipse case, the transitivity properties in this proposition means we need only consider when a parabola $D_\mu$ is $D_0$-good. The following proposition gives a necessary and sufficient condition for this to happen.

**Proposition 5.2.** Let $q$ be an odd prime power. The parabola $D_\mu$ is $D_0$-good if and only if $\mu$ is a nonsquare in $GF(q^2)$.

Proof. As discussed in the ellipse case, the transitivity properties from Proposition 5.1 show that $D_\mu$ is $D_0$-good if and only if no affine Baer subline through $(0,0)$ meets $D_\mu$ in two points. Suppose first that $\mu$ is a square, let $c$ be such that $c^2 = -\mu$, which exists since $-1$ is a square in $GF(q^2)$. Then $(0,c)$ and $(0,-c)$ are points on an affine Baer subline through $(0,0)$ that meets $D_\mu$ in two points. Hence $D_\mu$ is not $D_0$-good.

Now if $\mu$ is a nonsquare, let $R = (a,b)$ be a point of $D_\mu$, meaning $a = b^2 + \mu$. The affine Baer subline containing $(0,0)$ and $R$ consists of the points $\ell = \{(ta, tb) : t \in GF(q)\}$, and $\ell$ meets $D_\mu$ in a point distinct from $R$ if and only if $ta = (tb)^2 + \mu$ has a solution in $GF(q) \setminus \{0,1\}$. But since $ta = tb^2 + t\mu$, this is equivalent to $\mu = tb^2$ having a solution $t \in GF(q) \setminus \{0,1\}$, which cannot occur since $\mu$ is a nonsquare. Hence $D_\mu$ is $D_0$-good when $\mu$ is a nonsquare. 

**Corollary 5.3.** Let $q$ be an odd prime power. Then $AG(4,q)$ has a cap of size $2q^2$ lifted from two mutually good parabolas of $AG(2,q^2)$. 11
6 Larger Baer-caps

Given the results of the previous two sections, it seems natural to look for larger sets of conics whose union is a Baer-cap. Proposition 5.2 provides a particularly robust family of $\frac{1}{2}(q^2 - 1)$ Baer-caps mutually good with $D_0$, each of which is mutually good with about half of the other Baer-caps in the family. But unfortunately there does not seem to be a way to piece three of these parabolas together to make a Baer-cap. Computational results to find unions of three conics that form a Baer-cap have been generally negative, with one exception.

**Theorem 6.1.** Let $q$ be an odd power of 2, so that $q \equiv 2 \pmod{3}$. Let $\lambda \neq 1$ be a cube root of unity in $GF(q^2)$. Then $C_1 \cup C_\lambda \cup C_{\lambda^2}$ is a Baer-cap.

**Proof.** Since $q + 1 \equiv 0 \pmod{3}$, $\lambda^{q+1} = \lambda^{2(q+1)} = 1$, so by Corollary 4.5, the union of any pair of ellipses in $\{C_1, C_\lambda, C_{\lambda^2}\}$ is a Baer-cap. Letting $C = C_1$ and $D = C_\lambda \cup C_{\lambda^2}$, we can use Proposition 2.2 to show $C \cup D$ is a Baer-cap by showing $C$ is $D$-good and $D$ is $C$-good.

Any affine Baer subline $\ell$ meeting $D$ must meet either $C_\lambda$ or $C_{\lambda^2}$. Since $C$ is both $C_\lambda$-good and $C_{\lambda^2}$-good, this means $\ell$ cannot meet $C$ in two points, hence $C$ is $D$-good.

To show $D$ is $C$-good, we note that any affine Baer subline meeting $C$ meets each of $C_\lambda$ and $C_{\lambda^2}$ in at most one point, since these two ellipses are both $C$-good. By way of contradiction assume there exists an affine Baer subline $\ell$ which meets all three ellipses. Without loss of generality, we can assume $\ell$ meets $C_1$ in the point $(1,0)$. The line $\ell$ meets $C_\lambda$ in a unique point which we coordinatize as $(a+1,b)$, whence $\lambda = (a + 1)^2 + (a + 1)b + eb^2$.

If $b = 0$, we have $\lambda = (a + 1)^2$ which forces $\lambda^2 = a + 1$. A similar argument shows that $\ell$ meets $C_{\lambda^2}$ in the point $(\lambda,0)$. The points $(0,0)$, $(\lambda,0)$, and $(\lambda^2,0)$ lie together on an affine Baer subline only if $\lambda^2$ is a $GF(q)$-multiple of $\lambda$, which is not the case since $q \equiv 2 \pmod{3}$ meaning $GF(q)$ does not have a cube root of unity.

Thus we may assume $b \neq 0$, and as before let $c = a/b$ and write $\lambda = (c^2 + c + e)b^2 + b + 1$. The remaining points of $\ell$ are then coordinatized as $\ell = \{(ta + tb) : t \in GF(q)\}$, and one of these must lie on $C_{\lambda^2}$. Thus the equation $\lambda^2 = (c^2 + c + e)(tb)^2 + tb + 1$ must have a solution for some $t \in GF(q) \setminus \{0,1\}$.

Since $\lambda$ and $\lambda^2$ are nonidentity cube roots of unity, we have $\lambda + \lambda^2 = 1$. Thus the equation $(c^2 + c + e)(t^2 - 1)b^2 + (t - 1)b + 1 = 0$ also has a solution in $GF(q)$. Noting that $t^2 - 1 = (t - 1)^2$, we define $x = (t - 1)b$ from which it follows that $(c^2 + c + e)x^2 + x + 1 = 0$ has a solution in $GF(q)$. But the discriminant of the quadratic on the left is $c^2 + c + e$, which must have absolute trace 0 since the quadratic has the root $x$. However, $Tr(c^2) = Tr(c)$, so this implies $Tr(e) = 0$, a contradiction since $Tr(e) = 1$. 

12
Therefore, no affine Baer subline meeting $C$ can meet $D$ in two points, implying $D$ is $C$-good, finishing the proof.

**Corollary 6.2.** Let $q$ be an odd power of 2. Then $AG(4, q)$ has a cap of size $3(q^2 + 1)$ obtained by lifting a triple of pairwise-disjoint conics from $AG(2, q^2)$.

Using the same method as Corollary 4.5, it is not hard to show that the point $(0, 0)$ can also be added to the Baer-cap of Theorem 6.1 to obtain a larger Baer-cap. However, this addition makes clear that the caps obtained here are almost certainly identical to the caps discovered by Edel and Bierbrauer [5], though their construction originated from a coding-theoretic perspective.

### 7 Conclusion

The results in this paper provide several infinite families of caps in four-dimensional affine spaces and thus in their projective completions. Moreover, the results place the Pellegrino cap of $AG(4, 3)$ in the context of a robust family which includes the $(3q^2 + 4)$-caps of Edel and Bierbrauer. However, we cannot claim that these caps push the upper bounds. While the Pellegrino 20-cap is the largest in $AG(4, 3)$, the generalized Pellegrino cap in $AG(4, 4)$ has size 34, while the largest cap in $AG(4, 4)$ has size 40; see Edel and Bierbrauer [4]. In order to construct other caps from conics, one might consider exploring other pencils of conics. Our investigations concentrated on mutually interior conics as motivated by the work by Tucker [11] and only produced the caps demonstrated here.

### References


